



XLIX Legislatura

**DEPARTAMENTO
PROCESADORA DE DOCUMENTOS**

Nº 683 de 2021

Carpeta Nº 1734 de 2021 — Comisión Especial de innovación, ciencia y tecnología

---

TIPIFICACIÓN DE CIBERDELITO

Normas

MINISTERIO DEL INTERIOR

ASOCIACIÓN NACIONAL DE EMPRESAS ADMINISTRADORAS DE CRÉDITOS (ANEAC)

Versión taquigráfica de la reunión realizada el día 14 de octubre de 2021

(Sin corregir)

Presiden: Señores Representantes Gustavo Olmos, Presidente y Sebastián Cal, Vicepresidente.

Miembros: Señores Representantes Sebastián Cal, Diego Echeverría, Rodrigo Goñi Reyes, Miguel Lorenzoni, Martín Melazzi y señora Representante Lilián Galán.

Invitados: Por el Ministerio del Interior: señor Luis Alberto Heber, Ministro; doctor Guillermo Maciel, Subsecretario; Comisario Mayor licenciado Diego Fernández, Director de la Policía Nacional y doctor Ponce de León, asesor Letrado.

Por la Unidad de Ciberdelito: Comisario Mayor Paulo Rocha Martínez, Director y Subcomisario Winston Rodríguez.

Por la Asociación Nacional de Empresas Administradoras de Crédito (ANEAC): contador Luis Costa e ingeniera Mercedes Gatti.

Secretaria: Señora Myriam Lima.

═══════II═══════

SEÑOR PRESIDENTE (Gustavo Olmos).- Habiendo número, está abierta la reunión.

Buenos días a todos.

Ha sido remitido a esta comisión un proyecto de ley sobre Protección de los Derechos de los Niños, Niñas y Adolescentes en los Entornos Digitales. Esta iniciativa estaba en otra comisión y fue derivada a la nuestra; todos los diputados y diputadas deben tenerla en sus carpetas.

Estamos analizando un proyecto de ley presentado por varios legisladores sobre tipificación de ciberdelito para lo cual, en el día de hoy, estamos recibiendo con mucho gusto a una delegación del Ministerio del Interior, a fin de que nos dé sus comentarios y aportes sobre el tema, integrada por el señor ministro, Luis Alberto Heber; el subsecretario, doctor Guillermo Maciel; el director de la Policía Nacional, comisario mayor licenciado Diego Fernández; el director de la Unidad de Ciberdelito, comisario mayor Paulo Rocha Martínez; el subcomisario Winston Rodríguez, y el doctor Horacio Ponce de León.

Tenemos entendido que la delegación recibió el proyecto de ley y que tuvieron oportunidad de analizarlo.

SEÑOR MINISTRO DEL INTERIOR.- Es un gran gusto estar nuevamente en esta Casa, sobre todo, en esta instancia que es doblemente placentera, producto de que vemos una iniciativa legislativa de alto nivel, pues une a los partidos y trata de llenar un espacio vacío que se genera por la falta de normas. Para nosotros este tipo de iniciativas no solamente prestigian al Parlamento -felicito a los firmantes-, sino que nos ayudan en gran forma al combate a las nuevas formas de delito que, lamentablemente, existen en el mundo. Ustedes saben que, a esta altura, esta situación es motivo de preocupación entre las naciones. Podemos estar hablando de que las nuevas formas de guerra en el mundo son informáticas; entonces, estamos frente a todo un mundo distinto. La comisión y los miembros que firmaron el proyecto de ley nos ayudan a ver lo que se nos viene por delante.

En el Ministerio hemos creado la Dirección de Ciberdelito; ya teníamos la División de Delitos Informáticos, pero queríamos darle una jerarquía y una mayor importancia en el organigrama.

Quiero destacar que estoy acompañado por el subsecretario, el doctor Guillermo Maciel, quien conoce mucho del tema, quien también le ha dedicado tiempo a esta problemática, además del Director Nacional de la Policía. Asimismo, también estoy acompañado por el doctor Horacio Ponce De León, que es un entendido jurista, que hará un comentario de los artículos, además de contar con la presencia del comisario Rocha que está al frente de la Dirección de Ciberdelito y del subcomisario Winston Rodríguez, que ya tiene una experiencia muy extensa en delitos informáticos y que ahora quedó subsumido en lo que hoy es la Dirección de Ciberdelito.

Para nosotros, señor presidente y señores legisladores, este tema es muy importante; muy importante. Por lo tanto, con mucho gusto vengo a hablar y comentar acerca de este proyecto de ley porque me parece que son las cosas que trascienden el debate diario, la confrontación de ideas, que siempre son bienvenidas. Pero acá no puede haber confrontación de ideas; acá hay que advertir sobre una situación que no está debidamente contemplada en nuestra legislación, aunque hay normas desparramadas por todos lados. Justamente, el proyecto de ley intenta armonizar las normas y hacer un cuerpo legal único, a fin de que se pueda apelar al mismo con

novedades que para nosotros son trascendentes, que comentaremos en la medida en que vayamos analizando esta iniciativa.

Reitero que para nosotros es de vital importancia. Incluso, hay novedades que trascienden la legislación internacional. Acá nosotros tenemos que proteger a las personas, sus identidades y su privacidad. En este proyecto de ley hay una figura que determina que el uso o el mal uso de la imagen de otra persona es un delito. Creo que, de convertirse en ley, esta iniciativa nos pondrá en punta en lo que tiene que ver con la legislación internacional.

En este tipo de tema, vamos a tener que volver; no podemos prever todas las situaciones porque se van generando novedades a diario. Pero el mal uso del mismo, el uso que se da en las redes, el acercamiento, el abuso que pueda existir, es un motivo de preocupación de este Ministerio. El mal uso de una identidad robada -que es una novedad en este proyecto de ley- más lo que de alguna manera significa la utilización para amenazar, robar -como se roba- y muchos otros delitos -si quieren los podemos repasar-, lamentablemente, han crecido en esta materia de estafa informática.

Entonces, creemos que, de esta manera, se nos están dando herramientas para poder penalizar situaciones que para nosotros son preocupantes.

Si el señor presidente lo permite, quisiera ceder la palabra al señor subsecretario, que conoce bien este tema, le da la debida dimensión a este proyecto de ley y puede hacer comentarios al respecto.

SEÑOR SUBSECRETARIO DEL INTERIOR.- Buenos días, señor presidente y señores legisladores. Es un gusto estar en esta comisión.

Obviamente que compartimos y reafirmamos los planteos realizados por el señor ministro Heber, en cuanto a la importancia de una iniciativa de estas características. Vamos a señalar tres aspectos que nos parecen importantes.

Por un lado, desde el año 2004, está vigente el Convenio de Budapest sobre ciberdelitos, que ya fue firmado y está vigente en sesenta y cuatro países. En Latinoamérica, está vigente en Colombia, Argentina, México, Costa Rica y Chile, y en otras naciones de diferentes regiones. Nos parece muy importante adherir al Convenio de Budapest, ya que da instrumentos y legislación específica para combatir este tipo de delitos tan importante y que está en auge en el mundo entero.

En cuanto al Convenio de Budapest, ha venido informe del Ministerio del Interior; el informe ha sido favorable de las distintas unidades, entre ellas, Interpol y Dirección General de Lucha contra el Crimen Organizado; ha llegado a Cancillería -no está a estudio el tema, pero ayer, precisamente, en el acuerdo con el señor presidente, a la salida, nos cruzamos con el señor canciller, quien también se mostró favorable- y ahora, como me dice el ministro, pasó al Ministerio de Defensa Nacional. Así que el próximo pasó será, cuando llegue a Presidencia, que venga al Parlamento para que lo estudien los señores legisladores y eventualmente ratifiquen y adhieran al Convenio de Budapest.

Ese Convenio de Budapest -como seguramente va a relatar más adelante el subcomisario Rodríguez- tiene importancia en varios aspectos, pero uno que es fundamental es la cooperación internacional. Hoy el mundo funciona en base a la cooperación para el ataque a este tipo de delitos, ya que cuando uno es jaqueado no lo jaquean necesariamente desde nuestro país, sino que muchas veces es desde otro país donde se realiza el jaqueo u otro tipo de maniobras como las que están previstas en la legislación a estudio.

El segundo punto es que, como bien señalaba el ministro, se creó una unidad específica -la Unidad de Cibercrimen-, creada por resolución y está a consideración del Senado en la rendición de cuentas para darle rango legal, de forma tal de potenciar y poner en mayor jerarquía a esta Unidad de Cibercrimen y potenciar, a su vez, el Departamento de Delitos Informáticos; la idea es que en el futuro ambas unidades -Delitos Informáticos y Cibercrimen- se fusionen en una sola repartición, potenciando su trabajo. De esto nos van a hablar Rodríguez y Rocha posteriormente.

En cuanto al proyecto de ley del señor diputado Cal, fue objeto de estudio de la Gerencia del Área Jurídico Notarial del Ministerio del Interior, concretamente, del Departamento de Asesoría Jurídica, y luego formamos un grupo de trabajo, a cuya cabeza estaba el doctor Horacio Ponce de León -que hoy nos acompaña-, junto con otras profesionales, abogada y una escribana, para desmenuzar el articulado y pronunciarnos.

En ese sentido, vamos a dejar a la Comisión los dos informes -el de la asesoría jurídica del Ministerio del Interior y el del grupo de trabajo- con las recomendaciones. La opinión general en los dos informes -que se hicieron por separado- son coincidentes; ambos coinciden en apoyar el proyecto. Esa es la primera conclusión que sacamos: ambos participan de lo positivo que será este articulado en el combate a este tipo de delitos.

Lo que se agrega como eventualmente novedoso son antecedentes legislativos. En su momento, en la legislatura pasada, el senador Pedro Bordaberry y el senador De León -de diferentes partidos políticos, como es evidente- trabajaron en conjunto en una legislación muy similar. Prácticamente los mismos artículos; alguna novedad trae el proyecto del diputado Cal.

No dieron los tiempos legislativos, pero tenemos entendido -hemos hablado con estos exlegisladores- que en la legislatura pasada había consenso en las bancadas en avanzar en estos articulados. Como había artículos que presentaba De León y otros que presentaba Bordaberry, crearon un grupo de trabajo entre ellos y sus asesores y llegaron a consensos en algunos de esos artículos -combinando y teniendo artículos de consenso-, conciliatorios entre el texto del doctor Bordaberry y el del exsenador De León. Tomamos esos artículos -los conciliatorios- y también nos expresamos en algunos, manteniendo la redacción del proyecto del diputado Cal; en otros, sugiriendo alguna modificación, y en otros, inclinándonos por el texto conciliatorio.

Las variantes son muy pequeñas; son de redacción, de ajuste de texto, y obviamente quedan a consideración de ustedes para mejorar y perfeccionar el proyecto de ley.

Entrego a la Comisión los informes jurídicos.

Si le parece, señor presidente, nos gustaría escuchar las referencias que pueda hacer el doctor Horacio Ponce de León en nombre del grupo de trabajo.

Muchas gracias.

SEÑOR PONCE DE LEÓN (Horacio).- Es un gusto comparecer ante esta Comisión.

Voy a hacer algún comentario basado en el proyecto que recibimos para estudiar del diputado Cal. No sé si dará el tiempo para analizar todos los artículos.

El artículo 1º habla de lo que se llama "*Stalking* o acoso telemático". Nosotros vimos que algunas partes de ese artículo ya estaban incluidas en el proyecto, que comentó el señor subsecretario, del exsenador Bordaberry y del exsenador de León. En aquel proyecto, precisamente este delito, de acuerdo con cómo está descrito, ya estaba incluido

en lo que después fue aprobado como artículo 277- BIS del Código Penal que ya está vigente.

Entonces, sugerimos una modificación y agregamos a alguna parte del proyecto de Cal, de modo que quede en una unidad como el concepto de *grooming.* En realidad, como ya está vigente, lo que hicimos fue incorporar alguna parte del proyecto de Cal para lo que después podría ser agregado como artículo 278- BIS del Código Penal, y entonces quedaría redactado así: "El que valiéndose de las tecnologías de la información y comunicación difunda o publique imágenes u otras formas de representación con contenido sexual o erótico sin el consentimiento de la persona que resultare expuesta, será castigado con una pena de tres meses de prisión a dos años de penitenciaría".

(Diálogos)

——Resumiendo: este es un ejemplo de nuestro trabajo. En algunas partes del proyecto hicimos una pequeña modificación de redacción y en otras lo combinamos con aquel antecedente que teníamos del proyecto de Bordaberry, todo lo cual está expresado en el informe que se entregó a la Comisión. **SEÑOR PRESIDENTE.-** Muchas gracias, doctor Ponce de León. Sin duda, esos insumos serán material de trabajo de la Comisión.

SEÑOR MINISTRO DEL INTERIOR.- El doctor Horacio Ponce de León trató de ser breve a fin de dar posibilidad de hacer preguntas, pero toda la información está en el material que acaba de darles el señor subsecretario.

Antes de terminar nuestra exposición, nos gustaría que se escuchara al comisario mayor Rocha y al subcomisario Winston Rodríguez; me parece importante oír sus opiniones sobre el tema.

SEÑOR ROCHA (Paulo).- Es un honor haber sido convocado a esta sesión.

Como investigadores de delitos, podemos decir que -hablamos desde el terreno- para llevar a cabo una investigación es necesario tener los medios logísticos y los recursos humanos, pero es fundamental contar con legislación. El subcomisario Rodríguez tiene una muy larga trayectoria en investigación de este tipo de delitos. Todos los días hablamos, desde el terreno mismo, sobre el trabajo de detectar e investigar estos delitos y nos encontramos con un escollo importante en la legislación y en la obtención de información, la cooperación, ya sea nacional o internacional.

Como bien dijo el señor subsecretario, estos delitos pueden ser cometidos por una persona que está sentada en Europa jaqueando algo en nuestro país, con un servidor que está en Estados Unidos. Entonces, la prueba que los investigadores tenemos que seguir es la línea de la evidencia digital. Como esa línea de evidencia digital recorre todo el mundo, nos genera escollos importantes y demora en la persecución; a veces, ni siquiera se puede acceder a la información.

Por eso, nos parece fundamental tener herramientas jurídicas para este tipo de delitos.

SEÑOR RODRÍGUEZ (Winston).- Buenos días.

Hace catorce años que trabajo en Delitos Informáticos. Participe en la elaboración de proyectos de marcos legales en 2015 y 2017, pero no se concretaron. Me parece una idea muy interesante. Digo esto no solo como policía, sino como padre; aplaudo la gestión, porque mi hijo de nueve años podría ser vulnerable a los delitos informáticos.

En cuanto al proyecto, quiero decir que el fiscal se verá favorecido al tener un marco legal para su investigación y poder realizar tranquilo su tarea. Trabajamos en

investigaciones que a la postre se les cambió la tipificación por un tema de la analogía, ya que no existe en el Derecho Penal.

Es fundamental contar con la colaboración internacional. En este proyecto, ese aspecto no se contempla. Como decía el señor Maciel, sería bueno contar con el Tratado de Budapest; sería un complemento. Dicho tratado nos favorecería porque, en cierta forma, se obligaría a las empresas prestadoras de servicios de internet -Movistar, Dedicado, Claro y Antel- a preservar la información; hoy no todas la guardan por equis tiempo. Por ejemplo, si usted hace una investigación de una amenaza de muerte al presidente, cuando llegan las IP, las empresas prestadoras de servicios nos dicen que ellos no tienen identificado a quién fueron adjudicadas. Entonces, todo lo que se hizo por parte de la Policía, el desgaste hora- hombre y recursos, no logra nada. En cierta forma, obliga a las prestadoras de servicios de servidores, los *hosting,* a que tengan la información. Esa situación se da muchísimo cuando la persona que delinque realiza estafas electrónicas y utiliza servidores de Uruguay; ellos dicen: "No tengo resguardo; no sé a quién le adjudique esa IP". Delinquen utilizando servidores de Uruguay y nosotros no podemos saber qué fue lo que pasó.

Otra cosa interesante del Tratado de Budapest es que le permite al investigador o, en este caso, al fiscal poder congelar la investigación; poder congelar el usuario. Nosotros ya lo estamos haciendo con algunas empresas prestadoras de servicios. Por ejemplo, con Facebook; si se hace una investigación, nosotros, a través de una plataforma, podemos decirle a la empresa en Estados Unidos: "Congelame a este usuario por treinta días o ponémelo por noventa días en una lista de gris porque la Policía uruguaya lo está investigando". El Tratado de Budapest nos permite congelar y poder obtener la información, y que el fiscal trabaje tranquilo para que la investigación llegue a buen puerto. Todo esto es teniendo en cuenta el valor de la prueba; el valor de la obtención de la prueba. ¿Por qué? Porque -le pido disculpas al ministro por utilizarlo de ejemplo- si amenazo de muerte al ministro y no actuamos rápido, la evidencia digital se borra. Para que la Policía y la Fiscalía puedan trabajar mejor es fundamental contar con rápidas acciones y con marcos legales.

La educación que contempla este proyecto es fundamental, porque tenemos muchísima tecnología -Plan Ceibal, Plan Ibirapitá-, pero, a veces, nuestros adolescentes no la saben utilizar.

SEÑOR FERNÁNDEZ (Diego).- Mis comentarios serán muy básicos. Quiero resaltar algo importante. Dentro de la visión estratégica que elaboró la Policía Nacional para el año entrante, uno de sus objetivos es -planteados a través de esa visión- dar visibilidad a los que no tienen voz.

Convengamos que este proyecto -más allá de los ajustes que se le puedan hacer- es vital para darle protección a quienes no tienen voz en nuestra sociedad. Por lo tanto, es un objetivo estratégico de la Policía Nacional. Los delitos que se van a combatir son fundamentales para el desarrollo de las futuras generaciones.

SEÑOR REPRESENTANTE GOÑI REYES (Rodrigo).- Voy a dejar una constancia, ya que el ministro lo planteó; por supuesto que él lo sabe mucho mejor que nosotros. El gobierno planteó como prioridad la aprobación, por parte del Parlamento, del Convenio de Budapest. Está en las coordinaciones. La idea es votarlo, si están los informes -nos informaron que solo faltaba pasar por el Ministerio de Defensa Nacional-, este año, por lo menos, en la Cámara de Diputados, y probablemente en el Senado. El proyecto diseñado por el diputado Cal es muy importante y tiene sentido de cualquier manera. Como bien se planteaba, hay muchos aspectos que trascienden el propio convenio, pero quería dejar

constancia de que si no pasa nada raro -que esperemos no pase-, este Parlamento va a aprobar, el Uruguay va a aprobar el Convenio de Budapest en 2021.

SEÑOR REPRESENTANTE CAL (Sebastián).- Quiero saludar a la delegación y al señor ministro, si bien ya estuvimos conversando un rato fuera de la sala.

Primero que nada, quiero agradecer los comentarios sobre el proyecto; celebro que ustedes coincidan con los firmantes de esta iniciativa ya que existe la necesidad de contar con un marco legislativo que abarque todos los delitos que hoy están arriba de la mesa, aunque seguramente vayan a surgir más. Por tal razón, esto tiene que ser algo dinámico; el Poder Legislativo que está ahora y el que venga después tendrán que estar atentos para renovar, permanente, lo que aquí se establece. Sin duda, esta ley no va a permanecer diez años sin modificaciones.

Por otro lado, la cooperación internacional para poner en práctica esta iniciativa es tan importante como el proyecto en sí mismo. Si no adherimos al Convenio de Budapest, este proyecto no va a tener el mismo peso, y viceversa; si no contamos con un marco nacional, Budapest no va a recibir de nuestro país lo que espera. Por tanto, para el Convenio de Budapest también es muy importante que nosotros tengamos un marco jurídico claro -y nucleado- con respecto a este tema.

Hace pocos días, también adherimos a un convenio de cooperación internacional, lo que es muy importante, ya que no solo existe el Convenio de Budapest, sino varios.

Asimismo, celebro y felicito a las autoridades del Ministerio del Interior por tomar la decisión de crear la dirección específica de ciberdelitos; seguramente, el comisario Rocha y el subcomisario Rodríguez se han dado cuenta de la enorme tarea que tienen en esta materia.

Lo hemos dicho muchas veces: los delincuentes conocen mejor que nosotros la legislación de cada país, por lo que no es casualidad que hoy seamos el punto rojo de la región con respecto a este tema. Creo que Brasil fue uno de los últimos países en adherirse al Convenio de Budapest -lo hizo hace muy poco tiempo- ; tuvo que pasar por lo mismo que estamos pasando nosotros para entender la importancia de estar adherido a este Convenio.

Con respecto a los artículos 1º y 2º, se preguntaba por qué están separados el acoso telemático y el *grooming*; es porque yo creo que debemos tipificar como un delito el mero intento de acercarse a un menor, el más mínimo intento de acercarse a un menor de edad con cualquier tipo de fin repulsivo. Tal vez podamos hacer alguna modificación para que quede más claro, pero creo que es muy importante que el acoso telemático -o *stalking*- quede separado del *grooming.*

Por otro lado, creo que si la campaña nacional de educación no es lo más importante del proyecto, debe andar ahí; porque a uno no le vacían la cuenta porque sean *superhackers*, ni nada por el estilo; nos vacían una cuenta, nos vulneran la identidad, un correo electrónico o una red social, o un menor de edad intercambia un diálogo u otro tipo de información, por no tener una educación específica en el tema. Por ejemplo, a una señora le llegó un cupón -yo pongo siempre el mismo ejemplo- que dice que por un año va a tener un 50 % de descuento en una cadena de supermercados y se le pide que complete determinados datos, pero eso es algo que no pasa; a nadie le llega un cupón de un día para el otro sin haber participado en un sorteo, diciendo que ganó un auto o US$ 100.000. Sin embargo, a veces la gente, al no tener una formación específica sobre el tema, carga ciertos datos y después no hay absolutamente nada que hacer, y tampoco hay mucha responsabilidad por parte de quien también se ve afectado: es la banca privada. En realidad, a la gente le cuesta entender que lo que sucedió no es culpa

del banco; el primer afectado, sin duda, es el usuario, que se levanta un día y advierte que le falta tanta planta en la cuenta, que le vaciaron la cuenta o se entera de que su hijo está en una situación terrible, de la cual, como padre, no se dio cuenta, aunque estaba al lado suyo.

Son muchos los delitos que tipificamos; también hay uno que creo que es muy importante detectar para un desarrollo que nuestro país necesita: el terrorismo digital. Seguramente, el Ministerio de Defensa Nacional tenga buenas apreciaciones para hacer con respecto al terrorismo digital. Sin duda, es parte de lo que decía el ministro porque el mundo cambió, y las guerras, seguramente, tengan una pata digital muy importante.

Es importante tipificar el delito de terrorismo digital para darle protección a empresas que todos queremos que vengan a Uruguay, porque si no tenemos un marco jurídico que las proteja de cierto tipo de vulneraciones, no lo harán.

Yo me pregunto: ¿se puede hacer terrorismo digital? Por supuesto que se puede hacer. ¿Si yo vulnero el *software* de una intendencia y pongo todos los semáforos en verde, y se matan cinco personas, no estoy haciendo terrorismo?

Como dije al principio, este proyecto va a durar según lo que avance el mundo y cómo se vayan adaptando los delincuentes; sé que no es un proyecto para diez ni quince años. Sé que va a tener que sufrir modificaciones en forma permanente, y espero que así lo entiendan los que vengan después.

Los bancos privados también nos van a hacer llegar una propuesta -creo que todavía no lo hicieron- y tendremos que consultar con el Banco Central para saber qué opina; el Banco Central también está convocado a esta Comisión.

De todos modos, la opinión de ustedes también es muy importante; seguramente, el comisario Rocha y el subcomisario Rodríguez saben que se debe actuar con celeridad en materia de vulneración financiera, porque si nos vulneran la cuenta bancaria no pasan dos días hasta que se autoriza la transferencia a otro país, y para bloquear o congelar un fondo hay un proceso legal que se tiene que cumplir, que a veces es un poco impráctico para los tiempos que se manejan en las transferencias a través de la banca digital

La banca privada, cuando concurrió al Parlamento la semana pasada, nos hizo un planteamiento específico relativo a contar con la potestad de bloquear un fondo cuando vea algún tipo de acción sospechosa. Creo que eso sería algo muy importante, pero no sé qué pensará el Banco Central al respecto, y por eso su opinión va a ser indispensable para darle continuidad a esa propuesta.

También es muy importante la propuesta que ustedes realizaron, pero me gustaría que nos quedara claro cómo es el proceso que se lleva a cabo cuando se detecta alguna acción delictiva o la vulneración de una cuenta bancaria. Sería muy bueno que nos contaran cómo es el proceso, dónde se debe hacer la denuncia, qué tiempo hay entre que el usuario se da cuenta de que le falta plata en la cuenta y notifica el hecho, si el caso va a un juzgado, quién tiene que dar la orden, y si es un juez que tiene que bloquear los fondos.

Si nos pudieran explicar eso, sería muy bueno.

Muchas gracias.

SEÑOR REPRESENTANTE MELAZZI (Martín).- En primer lugar, agradezco al señor ministro y a los demás integrantes de la delegación por acompañarnos el día de hoy.

Simplemente, al igual que el señor diputado Goñi, quiero resaltar la importancia que tiene para Uruguay sumarse a este Convenio.

Me quedo con las palabras del subcomisario Rodríguez, sobre la importancia que tiene, como dice el artículo 16 del Convenio, la conservación rápida de datos informáticos almacenados. ¡Vaya si será importante! Hoy, en estos días, las tecnologías han avanzado tanto que creo que lo más difícil en los procesos de investigación debe ser, justamente, poder retener esos datos; los que llevan adelante este tipo de *hackeo*, por así decirlo, tienen clarísimo que cuanto antes se borre la información, más difícil es poder perseguirlos.

Entonces, apelo a que podamos sumarnos, señor presidente, a este Convenio de Budapest y que este proyecto de ley pueda ser una realidad.

Como bien decían, todos tenemos hijos o nietos y tenemos que ir pensando. Los tiempos corren y la verdad que día a día nos encontramos algún vecino que ha sido *hackeado* por abrir un archivo o de querer participar de una promoción -de una forma honesta- que termina en un daño que lo perjudica, no solamente a él, sino también a su familia y a todo el sistema financiero.

Felicitamos una vez más, agradecemos a la delegación y estamos a las órdenes.

(Ocupa la Presidencia el señor representante Sebastián Cal)

SEÑORA REPRESENTANTE GALÁN (Lilián).- Bienvenida la delegación.

Tengo algunas preguntas, ya que me quedaron dudas.

Obviamente, coincido con las palabras tanto del señor ministro como del diputado Cal, en que este tema que estamos tratando es tan dinámico que, en realidad, la legislación nunca va a alcanzar lo que es la tecnología aplicada a delinquir; por suerte, no solo se aplica a ello, sino a todos los usos de la vida. Me parece bien ir avanzando en esto.

Entiendo la importancia del Convenio de Budapest, pero me queda la duda de qué pasa si algo es delito en nuestro país -porque existe legislación al respecto- y en otro país no lo es. ¿Se puede juzgar o puede haber colaboración en ese sentido? El Convenio de Budapest abarca a los países firmantes del Convenio, no a todos los países, ¿no?

Otra duda que me quedó, de acuerdo con lo que dijo el doctor Ponce de León, tiene que ver con los artículos del Código Penal. Entendí que el doctor no se siguió explayando porque ya estaba el material que ustedes dejaron en la Comisión, pero igual me quedó una duda. Evidentemente, lo que él decía es que en el Código Penal vigente ya hay alguna legislación que está previendo esto que estamos tratando en este proyecto de ley. Entonces, quería que me explicara un poco esto del Código Penal; él decía que el *grooming* debía abarcar un artículo, el 278 bis del Código Penal, porque -según entendí- no estaba en ese momento incluido, por eso pregunto.

SEÑOR REPRESENTANTE LORENZONI HERRERA (Miguel).- Muchas gracias al señor ministro, al subsecretario y autoridades del Ministerio del Interior por estar aquí presentes.

No voy a redundar en lo que planteaba el diputado Cal, que lo hacía de forma muy exhaustiva sobre las cuestiones de fondo de este tipo de delitos, pero me gustaría hacer algunas preguntas concretas -quizás tengan respuestas o quizás me las puedan alcanzar en algún otro momento- a personas que entienden un poco más de estas cuestiones.

Asesorándome con personas que entienden más de estas cuestiones, me planteaban que algunos de estos delitos, en particular los contenidos en los artículo 1º,

2º, 5º, 6º y 7º, son propensos a ser cometidos a través de máscaras virtuales o de identidades falsas; entonces, se nos generaba la duda, al día de hoy, en este mundo en el cual se avanza tecnológicamente de forma tan vertiginosa y donde quienes cometen este tipo de delitos obviamente están a la punta de estas cuestiones, si el Ministerio cuenta con los recursos y la logística necesaria como para combatirlos de forma efectiva o tiene algún tipo de rezago, tanto desde el punto de vista de los recursos informáticos como de los recursos humanos, que son muy importantes en estos aspectos.

En segundo lugar, quisiera saber si el Ministerio identifica algún tipo de dificultades que hoy en el Uruguay dificultan canales de inmediatez para resolver este tipo de cuestiones, porque como bien se planteaba, el tiempo en este tipo de delitos es fundamental. Entonces, ¿cuáles serían los elementos que hoy, quizás, están generando dificultades en la inmediatez del tiempo y cuáles podrían, desde el punto de vista de la legislación local -porque acá hay un componente también de legislación internacional-, mejorar un poco el tema de los tiempos?

Por último, en base a las denuncias que el Ministerio del Interior habitualmente recibe por este tipo de delitos que no están tipificados pero que la gente obviamente denuncia, quisiera saber si hay un estimativo de cuántas denuncias se reciben por este tipo de delitos y por las figuras penales que se están creando a partir de este proyecto.

SEÑOR MINISTRO DEL INTERIOR.- Haré algunos comentarios generales porque las preguntas son muy específicas; naturalmente, iremos dando la palabra para que sean respondidas por los especialistas.

Simplemente y a modo de introducción en las respuestas, quería señalar nuestra alegría en cuanto al compromiso de que el Convenio de Budapest se firme cuanto antes. Nosotros hemos insistido en el Poder Ejecutivo aunque las jurídicas a veces se toman su tiempo -es lógico- para analizar, pero estábamos un poco ansiosos de tener este instrumento del Convenio de Budapest que, para nosotros, es fundamental. Simplemente, quería mencionarlo.

Asimismo, quiero señalar respecto a la intervención del señor diputado Cal -que ahora está presidiendo la Comisión- que sí, hay nuevas formas que aparecen todos los días, como él expresaba. El terrorismo cibernético existe.

Hace unos días leía un artículo en una revista especializada que decía que ahora las amenazas entre países son de introducción de virus; pueden hasta parar la energía eléctrica de un país y están amenazados en ese sentido. Hay amenazas cibernéticas de parar la producción.

Entonces, estamos frente a un mundo muy distinto. Alguno dirá que en Uruguay no pasa nada. Sí, no pasa hasta que desde el lugar más recóndito del mundo alguien se pregunta por este país. Y hemos tenido accidentes informáticos.

En Identificación Civil nosotros estamos haciendo una inversión muy grande, para *aggiornar* todos los equipamientos y para generar situaciones de mayor protección a la base de datos. Es una base de datos que es la población del Uruguay; y además tiene un valor, porque eso puede ser de interés comercial. La información hoy vale. Por lo tanto, nosotros tenemos que tener conciencia de lo que viene. Hemos tenido episodios que se están investigando, como ha trascendido, en la base de datos de Antel.

Estamos muy preocupados con esta situación. Por suerte, nosotros nos adelantamos a esta situación con la dirección de cibercrimen. No es ciberdelito; es cibercrimen, yo me equivocaba en alguna referencia. El cibercrimen es un tema que llegó para expandirse, en la medida de la imaginación. Fíjense: estaba comentando con el

subcomisario Rodríguez y con el comisario Rocha que tuvimos un menor que cometió cuarenta y cinco delitos, y también me estaban diciendo que agarraron a tres menores en Treinta y Tres. Tienen una capacidad realmente increíble; es una invitación al delito por la facilidad que encuentran para generar la penetración en lo que puede ser un posible *hackeo* a cuentas o para la estafa. Por lo tanto, tenemos que actuar rápido en esto, por eso nuestras ansiedades.

Para contestar las preguntas de los señores legisladores, solicitaría que hagan uso de la palabra tanto el comisario Rocha como el subcomisario Rodríguez; después correspondería que el doctor Ponce de León pudiera responderle a la señora diputada.

SEÑOR RODRÍGUEZ (Winston).- En cuanto al tema de las estafas electrónicas, hay diferentes modalidades.

Partamos de la base que obtener dinero de cualquiera de los que estamos acá es relativamente fácil para el que tiene conocimiento; lo hacen mediante *fishing*, mediante engaño, que es en lo que se basan. La pesca se dio muchísimo este año. Inclusive, empresas prestadoras de servicios, puntualmente Redpagos, fueron víctimas muchísimas veces del *fishing.* ¿Qué es lo que hace la Policía en este caso? Primero abordamos a la víctima. La víctima viene, se presenta, tomamos denuncia, le damos cuenta al fiscal y le pedimos al banco que tenga en consideración darnos tiempo -que es lo que decía el señor diputado Cal- para que se pueda preservar, congelar o retener esa cuenta mientras nosotros hacemos la investigación inmediata.

Lógicamente, algo fundamental que tienen los delitos informáticos es la trazabilidad del delito. Hoy -lo decía el comisario Rocha cuando se presentó y es algo que yo pongo de ejemplo cuando doy charlas- ustedes son uruguayos y tienen plata en un banco argentino, pero el banco argentino utiliza servidores de Estados Unidos y quien los *hackea* a ustedes es un ruso, un americano o de cualquier país. Entonces, tenemos que realizar una investigación en cuatro países; por ende, existe la cooperación internacional y nosotros pedimos hacer las actuaciones rápidamente. Lo importante es obtener la información rápido y para eso necesariamente también tenemos que pedir colaboración al banco, que es que intercepta o el que hace el giro del dinero. Entonces, es fundamental actuar rápido y tener contacto para hacer eso en el banco.

SEÑOR ROCHA (Paulo).- Con respecto a la consulta de los recursos -en mi primera intervención lo había puntualizado-, son necesarios recursos humanos y especialistas en el tema, con las dificultades que a veces representa tener y preservar especialistas, principalmente en este tema de la ciber seguridad, porque la actividad privada tiene mucha necesidad de estos especialistas y los absorbe.

En cuanto a los recursos logísticos, nosotros estamos siempre mirando los recursos con los cuales se cuenta en la región. Por ejemplo, en Sudamérica hay países que realmente tienen grandes infraestructuras logísticas dedicadas al cibercrimen. Hay países, como Colombia, que tienen edificios enteros solamente para el cibercrimen.

A nivel nacional, es importante también reportar los incidentes, porque a veces pasa que muchas instituciones privadas, para no ver afectada su imagen de empresa, no reportan los incidentes y se desconoce. A veces recomponen al usuario lo perdido y eso complica obtener la información completa o ver la magnitud de la problemática.

SEÑOR MINISTRO DEL INTERIOR.- Si los convenios internacionales no están firmados, notoriamente, los países no están obligados a cooperar. Podemos, por relaciones diplomáticas, pedir que lo hagan, pero es así.

Creo que ya hay sesenta y cuatro países que firmaron, y entre ellos están los más importantes en cuanto al manejo informático, que participan un poco de esto; o sea que entramos un poco en el mundo que puede generar esta situación. Simplemente, quería hacer ese comentario a la señora diputada.

Sobre el tema de recursos, para ser claros, son insuficientes; nosotros los precisamos. En la rendición de cuentas presentamos un artículo que nos posibilita el destopeo para contratar gente especializada que nos pueda ayudar. Ahí tenemos un riesgo. ¿Por qué? Porque por más destopeo que haya, el Estado no paga lo suficiente para retener gente realmente especializada que en el mercado a veces se paga el doble. Comentábamos con el señor subsecretario el caso de uno de los analistas principales de la Agesic que se fue porque le triplicaron el sueldo. Creemos que el Estado tiene que hacer alguna excepción al respecto. Nosotros pedimos el destopeo, pero notoriamente el destopeo no es suficiente. Esto es para darle apoyatura tecnológica.

Inclusive, hay distintos tipos de *hackers* en el mundo. Está el *hacker* blanco, el *hacker* gris y el *hacker* negro. Yo me estoy enterando de esto ahora. El blanco es un buen *hacker*; el gris a veces comete delitos, pero también ayuda; y el negro comete delitos de todo tipo. Eso me lo enseñó gente que sabe más que yo, en entrevistas que he tenido respecto a este proyecto; uno va aprendiendo sobre esto.

(Ocupa la Presidencia el señor representante Gustavo Olmos)

——Simplemente, quiero mencionar que nosotros tenemos idea de proveer algunos recursos. Hoy los recursos son insuficientes como para dar apoyatura técnica a nuestra Dirección, con la que estamos muy conformes, porque la verdad que nuestro Departamento de Delitos Informáticos primero, y ahora la Unidad de Cibercrimen tiene prestigio. Quiero reconocer, inclusive a los oficiales que nos acompañan, porque he tenido, como ministro, buen retorno de la acción que han tenido los policías que han actuado frente a delitos informáticos, por el protocolo que llevan adelante y por la capacidad profesional que están poniendo; muchos casos se han resuelto, no todos. Simplemente, lo digo como información porque, a veces, no tenemos los recursos suficientes -poco más que un escarbadientes-, pero tenemos un material humano importante que nos ayuda a hacer la investigación correspondiente.

Si me permite, señor presidente, pido al señor subsecretario y después el doctor Ponce de León que terminen de contestar las preguntas.

SEÑOR SUBSECRETARIO DEL INTERIOR.- Hago un apunte para complementar la respuesta a la señora diputada en cuanto a la persecución del delito penal. Ya está previsto en nuestro Código Penal, en el artículo 9º, que los delitos cometidos en el territorio de la República serán castigados con arreglo a la ley uruguaya -de ahí la importancia de que tengamos legislados estos delitos-, fueren los autores nacionales o extranjeros, sin perjuicio de las excepciones establecidas por el derecho interno y por el derecho internacional. A esto se le suma la figura de la extradición. Entonces, el delito lo cometieron acá, *hackearon* la cuenta del banco, usurparon su identidad, y está la persecución internacional a través del instituto de la extradición si se da con los responsables para traerlos y juzgarlos en el Uruguay, salvo que el país o la isla no tengan tratado de extradición. Hoy, en general, la inmensa mayoría de los países tienen tratado de extradición y la cooperación internacional funciona fantásticamente en esta materia.

SEÑORA REPRESENTANTE GALÁN (Lilián).- Yo le preguntaba porque me han comentado de gente que hace una denuncia, por ejemplo, de niños jugando en una plataforma, que después no puede hacer el seguimiento porque -yo no sé mucho de esto; tengo asesores- el país en el que está esa otra persona jugando en línea con los niños no

es Uruguay. Por eso decía: el delito puede ser acá en Uruguay pero en ese otro país puede no serlo. Entonces, si no está comprendido dentro del Convenio de Budapest, ¿qué se puede hacer en esos casos? Me imagino que no se podrá dar seguimiento. Como decían ustedes, capaz que eso después se borra de la línea. ¿Qué posibilidad tiene la legislación uruguaya de alcanzar esos casos? Esa era concretamente la pregunta, no sé si se entendió.

SEÑOR SUBSECRETARIO DEL INTERIOR.- Hay que analizar cada caso concreto. En forma general, el 99 % de los delitos son perseguibles. Podrá haber casos excepcionales en los que, cuando se hace el pedido de extradición, se entiende por parte del otro país que no es un delito y defiende a su connacional, pero en la mayoría de los casos, por suerte, no funciona, y mucho más si se firma el Convenio de Budapest que nos da la posibilidad de ingresar, por ejemplo, a los servidores de la empresa -como señalaba el subcomisario Rodríguez-, ver la IP y saber de qué computadora o instrumento digital partió y quién es su titular.

SEÑOR PONCE DE LEÓN (Horacio).- Con respecto a lo que se preguntaba acerca del proyecto y el Código Penal, en general el proyecto consiste en modificar o incorporar ciertas disposiciones al actual Código Penal, agregándole incisos o insertando artículos. Generalmente, cuando se insertan artículos al Código Penal en un número de artículo que ya existe se hace otro artículo con el mismo número y se le pone bis. Eso pasa tanto en este proyecto como en el que se había trabajado antes, pero sucedió que una de las propuestas trabajadas en la anterior legislación fue recogida y se encuentra en el actual artículo 277 bis del Código Penal por una ley de 2017. El Código dice artículo 277 bis pero no le pone nombre, es lo que está tratado como *grooming*, o sea que eso ya está contemplado. Lo que pasa es que este asunto se recogió aisladamente; ahora, con el proyecto, ya el problema se trata de forma más orgánica.

SEÑOR PRESIDENTE.- Agradecemos la documentación que nos enviaron. Somos conscientes de que para la plana mayor del Ministerio del Interior estar acá durante una hora es un gran esfuerzo. Agradecemos enormemente los materiales escritos, que nos ayudan mucho.

Por cualquier cosa estaremos intercambiando nuevamente.

SEÑOR MINISTRO DEL INTERIOR.- Estamos a las órdenes de la Comisión para cualquier modificación. Confiamos en el trabajo de los legisladores. Sé que es intenso y muy bueno; ojalá que tengamos este instrumento cuanto antes.

(Se retiran de sala las autoridades del Ministerio del Interior) (Ingresa a sala una delegación de la Asociación Nacional de Empresas Administradoras de Créditos)

SEÑOR PRESIDENTE.- La Comisión Especial de Innovación, Ciencias y Tecnología tiene el gusto de recibir a la Asociación Nacional de Empresas Administradoras de Créditos, representada por el contador Luis Costa y por la ingeniera Mercedes Gatti.

Los hemos invitado, porque nuestra Comisión está analizando un proyecto de ley impulsado por el señor diputado Sebastián Cal y firmado por varios legisladores sobre la tipificación de algunos ciberdelitos. Entre los actores cuya opinión nos parecía relevante, está la de la Asociación Nacional de Empresas Administradoras de Créditos, así que si les parece, les cedemos el uso de la palabra.

SEÑOR COSTA (Luis).- Agradecemos a la Comisión Especial de Innovación, Ciencia y Tecnología por esta invitación a Aneac para opinar sobre el proyecto a estudio de tipificación del ciberdelito.

Nos gustaría poder comenzar por presentar a nuestra Asociación, Aneac, que es la Asociación Nacional de Empresas Administradoras de Créditos.

Esta Asociación fue creada hace muchos años por empresas que se dedican a otorgar créditos, pero que no son instituciones bancarias. Se dedican, principalmente, a otorgar préstamos a las familias. Su actividad es muy importante y está supervisada por el Banco Central del Uruguay.

Voy a dar algunos números solo para ubicarnos en lo que somos.

La cartera total de créditos otorgados por instituciones financieras reguladas por el Banco Central es de aproximadamente US$ 15.600.000.000. Alrededor de US$ 6.400.000.000 son créditos a la familia: 40 % para vivienda, 3 % para autos y 57 % para el consumo de las familias uruguayas por necesidades de financiamiento que estas tienen. El 50 % es cubierto por el BROU y el BHU y el otro 50 % por las instituciones privadas. De estas, 30 % son bancos privados y el 20 % restante son estas empresas financieras no bancarias.

O sea que las empresas financieras no bancarias representan el 20 % del total del crédito a las familias en el Uruguay, pero por las características de sus créditos, representan más del 50 % del crédito a las familias en pesos nominales.

Si lo analizáramos según el número de clientes, las empresas financieras no bancarias que reportan al Banco Central atienden a más de 1.120.000 personas. En realidad, tienen más clientes que todos los bancos juntos, incluidos los oficiales.

Es importante destacar que, según el análisis de la Central de Riesgos Crediticios del Banco Central, hay 520.000 uruguayos que solo tienen saldos activos con empresas como las nuestras. O sea que el 33 % de la población de Uruguay tiene financiamiento solo con las empresas financieras no bancarias. Hay 450.000 personas que solo se atienden en los bancos, 520.000 que solo se atienden por empresas como las nuestras y 600.000 que se atienden en ambos.

Las características de los créditos de las empresas financieras no bancarias es que son montos mucho más chicos, por lo que hay una cantidad impresionante de operaciones que podrían estar sujetas a los peligros del ciberdelito. Por ejemplo, los bancos tienen un crédito promedio de $ 173.000, en tanto las empresas financieras no bancarias, tienen uno de $ 22.000.

Incluso, si depuramos los $ 173.000, que es el promedio de de los créditos hipotecarios de los bancos para viviendas y automotores, daría aproximadamente $ 85.000, lo cual igual es casi cuatro veces más alto que lo de las empresas que nosotros llevamos adelante; así que hay involucrada una cantidad muy importante de gente.

Manejamos operaciones con más de más de 1.100.000 personas, con lo cual este tipo de ciberdelito nos puede afectar en forma muy importante.

En relación al proyecto, nuestros técnicos nos han destacado, en primer lugar, la unificación de la regulación referente a ciberdelitos y la claridad del proyecto.

En segundo término, que tiene como referencia la regulación internacional más relevante en el tema, que es el Convenio de Budapest.

En tercer lugar, nos han destacado en forma muy fehaciente el tema de la novedad y la innovación en materia de educación sobre el manejo de las finanzas personales y la ciberseguridad como un punto muy positivo.

En relación a algún punto negativo, nos informaron que algunos profesionales en materia penal que han opinado sobre el proyecto de ley lamentan que no sugiera adherir

al convenio de Budapest y que, al no adherir, no se acceda a una serie de mecanismos de cooperación internacional previstos en dicho convenio que serían de gran utilidad para el combate del ciberdelito.

La realidad es que las empresas asociadas a Aneac, al no tener depósitos ni dinero de sus clientes, como los bancos, son menos propensas a sufrir ciberataques y los casos que hemos tenido o estudiado están contemplados en los tipos personales que el proyecto cree. O sea que, por nuestra parte, tenemos una visión favorable sobre el proyecto.

Cedo el uso de la palabra a la ingeniera Gatti, que puede tener una visión más técnica del proyecto.

SEÑOR PRESIDENTE.- A modo de aclaración, el convenio de Budapest está siendo objeto de otro trámite parlamentario en paralelo. Por eso, no está incluido en este proyecto, pero está en las puertas de ser aprobado por el Parlamento.

SEÑORA GATTI (Mercedes).- Soy Mercedes Gatti. Quiero agradecerles la invitación de poder estar acá y dar nuestra opinión respecto a esto.

En primer lugar, me parece magnífico este proyecto que se está evaluando. Creo que es súper necesario por el momento en el que estamos; así que los felicito por poner esto sobre la mesa y darnos también la posibilidad de brindar nuestra opinión.

En lo que tiene que ver con la tipificación de ciberdelitos, estamos de acuerdo. Simplemente, voy a hacer algunos comentarios o consideraciones que se me vinieron a la mente cuando leí este proyecto de ley para que lo tengan sobre la mesa y lo puedan analizar. En primer lugar, la duda que tengo es cómo se va a hacer la cooperación entre los distintos gobiernos o países. Como saben, Internet no tiene fronteras y los ciberdelitos pueden iniciarse en un país, continuar en otro y terminar en Uruguay, o al revés.

Reitero que me gustaría saber cómo va a ser la cooperación entre los distintos gobiernos y países si Internet no tiene fronteras y los ciberdelitos pueden iniciar en un lugar, continuar en otro y finalizar en otro país. Entonces, ¿cómo vamos a cooperar internacionalmente con los distintos gobiernos? Esta es una duda que me surge al leer el proyecto de ley y que me parece interesante poder incluir qué medidas vamos a tener de cooperación.

Por otro lado, cómo vamos a validar y a probar que estamos ante un determinado delito, y quiénes son los responsables de poder dar ese veredicto, es decir, quién determinará que un delito que es de tal naturaleza y quiénes son los responsables de él. A veces, los ciberdelitos son muy confusos y, de hecho, hay muchos de ellos que pasan por las distintas tipologías; entonces, si estoy ante un delito que puede ser daño informático, a su vez, acceso ilícito a la información y, a su vez, vulneración de datos, ¿con cuál de ellos me voy a regir si está pasando por todos ellos? Un ejemplo de ello, que es simple: uno de los ataques más conocidos en el día de hoy, es el *ransomware*, que va a través de la ingeniería social, que puede llegar por correo electrónico y que el funcionario de la empresa hace doble clic y se infecta con ese *ransomware* y se inscripta toda la información del equipo y de la red. Ahí hay varios delitos: tenemos daños informáticos, vulneración de datos, acceso ilícito. Entonces, ¿en cuál lo voy a categorizar? ¿Cuál va a ser la naturaleza y la pena? ¿Se suma la pena de los tres o se considera el delito mayor? Esta es una duda que me surgió y estaría bueno analizar la posibilidad de poder incorporarlo.

Otra de las cosas que surge es la posibilidad de incorporar la necesidad de actualización de manera periódica de todo esto. Como saben, esto cambia minuto a

minuto. Por tanto, habría que establecer un período de revisión y de actualización porque, a medida que vamos avanzando, aparecen nuevos delitos o formas de vulnerar todo lo que tiene que ver con la informática. Por tanto, creo que es bueno incluir un período de actualización.

Lo otro que me llamó la atención es lo referido a ataques de denegación de servicios. No lo vi pero también ha ocurrido en Uruguay, sobre todo, en la banca, por lo que me parece que puede ser incluido como otro ciberdelito. Insisto que estos son comentarios o dudas que me surgieron a partir de la lectura del proyecto de ley. Me parece magnífico que estemos ante una iniciativa como esta porque me parece que es supernecesaria en los tiempos en que estamos.

SEÑOR REPRESENTANTE CAL (Sebastián).- Antes que nada, quiero saludar a la delegación. Agradezco las apreciaciones sobre el proyecto de ley. Entendemos que esta es una iniciativa muy necesaria y oportuna.

Arranco por el final. No me quedó claro eso de delito ataque de denegación de servicios. Sería bueno si ustedes nos pudieran hacer llegar algunos aportes como prefieran, tal vez por escrito, a través de la secretaría de la comisión.

Sin duda que este proyecto de ley sin Budapest le falta una pata, pues es muy importante porque sin la cooperación internacional es indispensable para el combate a la ciberseguridad. Ya hemos sumado hace muy pocos días una cooperación internacional en lo que era Iberoamérica si mal no recuerdo. El estar incluidos en Budapest es tan importante como el proyecto de ley en sí mismo. En lo personal, creo que lo que va a favorecer la ciberseguridad es la campaña nacional de educación, orientando a la gente hacia buenas prácticas de manejo que hoy no tiene. Todos sabemos que si bien hay una inclusión financiera obligatoria que ya está derogada, la gran mayoría de la gente sigue bancarizada y hoy la banca digital tiene más peso que la banca física. De hecho hay bancos que están operando solamente de forma digital y están prosperando y aumentando sus ingresos de forma exponencial, por lo que ello seguirá motivando a los bancos para seguir trabajando en la modalidad digital. Sería muy raro que algún banco no lo hiciera.

Así que estoy de acuerdo en orientar a la gente hacia las buenas prácticas de manejo porque es indispensable; ese será el principal combate a los ciberdelincuentes, lo que va a favorecer la seguridad de todo un país.

Después hay otros puntos que tal vez no sean de gran interés específico del rubro de quienes nos visitan, pero no menos importantes, que promueven el desarrollo y la promoción de inversiones en nuestro país como es el combate al terrorismo digital y demás.

SEÑOR REPRESENTANTE MELAZZI (Martín).- Muchas gracias por comparecer ante la comisión.

Simplemente quiero saber si ustedes han detectado algún tipo de ciberataques o ciberdelito que nos puedan contar. Por ejemplo, uno de los problemas que nos relataba la Asociación de Bancos Privados es que la actual legislación no les permite congelar los fondos de las cuentas de los *hackeadores* de forma automática. Quisiera saber cuál es la opinión que ustedes tienen al respecto.

SEÑOR COSTA (Luis).- En ese sentido, nosotros tuvimos una diferencia muy importante con la asociación de bancos pues no tenemos depósitos de la gente por lo que no sufrimos ese inconveniente. Como empresas hemos sufrido ciberdelitos que, hasta ahora, se han arreglado con las tipificaciones que se podían hacer con el régimen

anterior, ya sea por el lado del fraude o por otros mecanismos. Estimamos que ahora, al estar tipificado este tipo de delitos, será mucho más sencillo poder hacerlo porque antes estaba el desafío de demostrar que eso era un fraude cuando realmente era un ciberdelito típico.

SEÑORA GATTI (Mercedes).- Yo estoy en Anda, soy la gerente general de la información; hace dos meses que estoy ahí. Estuve diez años como CEO del BBVA Uruguay y dos años trabajando en el exterior, en España para la casa corporativa de BBVA. En Anda no puedo contar mucho porque, en realidad, hace muy poco que estoy trabajando allí. Por suerte en estos dos meses no hemos tenido nada relevante. Las cosas que he visto en mi trayectoria en Uruguay fueron: *phishing, ransomware,* ingeniería social. También he visto algún ataque más complejo. En mi experiencia en España y trabajando con distintos países, he visto ataques más complejos; con ello podríamos estar un buen rato conversando. Pero, en Uruguay, hubo ingeniería social, envíos de correos con engaños intentando que se van transferencias hacia otros lados, fraudes al CEO, suplantación de identidad, *phishing, ransomware*. También hubo algún caso un poco más complejo en alguna procesadora, alguna cosa como la obtención de datos de tarjeta y todo lo que tiene que ver con a parte de clonación *skimming* y lo demás, también es superconocido, pero de mi período actual no puedo contar mucho porque hace poco tiempo que estoy ahí.

SEÑOR PRESIDENTE.- La Comisión agradece vuestra comparecencia; quedamos a las órdenes a través del canal de secretaría para aportar algún otro insumo que entiendan pertinente, en particular lo que el diputado Cal solicitaba en cuanto al ataque de denegación de servicios. Seguiremos trabajando y, eventualmente, podremos enviarles una nueva versión del proyecto de ley cuando haya avanzado en comisión.

(Se retira de sala la Asociación Nacional de Empresas Administradoras de Crédito)

——Se pasa a intermedio por tres minutos.

(Es la hora 11 y 30)

——Continúa la reunión.

(Es la hora 11 y 38)

——De acuerdo con lo conversado en la Comisión, Presidencia y Secretaría coordinarán con las delegaciones para elaborar una agenda que nos permita agilizar el tratamiento del proyecto.

No habiendo más asuntos, se levanta la reunión.

≠